1) ¿Qué tipo de firma digital permite detectar cualquier cambio posterior de los datos firmados y se genera mediante un dispositivo seguro de creación de firma?

a) Avanzada.

b) Ordinaria.

c) Con árbitro.

**d) Reconocida.**

2) ¿Cuál de las siguientes es una autoridad de certificación española?

a) VeriSign.

**b) FNMT.**

c) Comodo.

d) Thawte.

3) ¿Qué medidas físicas de seguridad incluye el DNIe?

a) PIN.

b) Cifrado de los datos del chip.

**c) Relieves.**

d) Ninguna de las anteriores.

4) ¿Qué tipo de certificado es el más extendido?

a) PEM.

**b) X.509.**

c) X.506.

d) DER.

5) Los certificados digitales se crearon para solucionar el problema de...

**a) Confianza en la clave pública de un usuario.**

b) Gestión del anillo de claves públicas.

c) Pérdida de la clave privada.

d) Confianza en la clave simétrica de un usuario.

6) ¿Cómo se denomina el mecanismo que permite consignar el momento exacto en que se ha realizado la firma?

a) Sincronismo de tiempo.

b) Estampado de hora.

**c) Sellado de tiempo.**

d) Ninguna de las respuestas es correcta.

7) ¿Qué servicios proporciona la firma digital?

a) De autenticación.

b) De integridad.

c) De no repudio.

**d) Todas las respuestas son correctas.**

8) ¿Cómo se llama el sistema que permite el intercambio de claves en SSL/TLS?

a) RSA.

**b) Diffie-Hellman.**

c) DSA.

d) ElGamal.

9) Bitlocker es un ejemplo de...

a) Cortafuegos.

**b) Tecnología de cifrado de disco para Windows.**

c) Antivirus.

d) Sistema de firma digital.

10) ¿En qué consiste la fase de comunicación de SSL/TLS?

a) En intercambiar los nombres de las aplicaciones que se conectan.

b) En la presentación de los participantes en la comunicación.

c) En el intercambio de claves públicas y la negociación del algoritmo de cifrado.

**d) En cifrar el tráfico con cifrado simétrico.**

11) ¿Cuál de las siguientes afirmaciones sobre el correo electrónico no deseado y el correo basura o spam es cierta?

a) Es más fácil detectar el correo electrónico no deseado que el correo basura o spam.

**b) Es más fácil detectar el correo basura o spam que el correo electrónico no deseado.**

c) Un correo electrónico que anuncia un producto para prevenir el envejecimiento de la piel enviado a personas que no han solicitado recibir ese tipo de información se considera correo electrónico no deseado.

d) Ninguna de las respuestas es cierta.

12) ¿Cuál de las siguientes afirmaciones relacionadas con la suplantación de la identidad es falsa?

a) El pharming es una técnica de suplantación de identidad que consiste en redireccionar peticiones a una página web falsa.

b) El correo electrónico es una herramienta muy utilizada por los estafadores para embaucar a las víctimas.

c) En la mayoría de los casos las víctimas no son conscientes del engaño, por lo que no dudan en introducir su contraseña en una página web que no es legítima pensando que sí lo es.

**d) El vishing consiste en el envío de mensajes de texto a la víctima para procurar que visite una página web o llame a un número de teléfono.**

13) ¿Cuál de las siguientes opciones constituye un ejemplo de ingeniería social aplicada a la informática?

a) La creación de una página web que imita el funcionamiento de la web de otro portal web para obtener las claves de acceso de los clientes.

b) El envío de un correo electrónico suplantando la identidad del banco y en el que se indica que se ha detectado un problema y que se debe llamar a un número de teléfono que aparece en el correo para solucionarlo con la mayor brevedad posible.

c) El envío de un correo electrónico en el que se indica que se ha ganado un premio (sin haber participado en ningún sorteo) y que tenemos que visitar un enlace que se nos facilita en el correo para recoger dicho premio.

**d) Todas las opciones anteriores son correctas.**

14) ¿Cuál de las siguientes opciones contribuye a evitar los fraudes informáticos derivados de las cadenas de correos?

a) Desconfiar de los correos electrónicos de desconocidos.

b) Al reenviar masivamente un correo electrónico, eliminar las direcciones de correo a las que este se ha enviado previamente.

c) Al reenviar un correo a mucha gente, utilizar el campo de correo en copia oculta (campo CCO) en lugar del destinatario (campo Para).

**d) Todas las respuestas anteriores son correctas.**

15) La página de inicio de nuestro equipo ha cambiado automáticamente. ¿Por qué variedad de software malicioso es probable que esté infectado?

a) Virus.

b) Gusano.

**c) Browser hijacker.**

d) Keylogger.

16) ¿Cuál de las siguientes opciones es verdadera?

a) Un keylogger es un tipo de software malicioso que captura las pulsaciones de las teclas.

b) El hecho de descargar un programa de su página web oficial no garantiza que este no sea software malicioso.

c) Conviene desconfiar del software que circula por las redes P2P porque desconocemos su procedencia.

**d) Todas las opciones anteriores son verdaderas.**

17) ¿Cuál de las siguientes afirmaciones sobre la denegación de servicio es verdadera?

a) Se produce solo en servidores web y servicios accesibles por la red.

**b) El hecho de que el personal de limpieza desconecte accidentalmente un equipo informático que está funcionando puede ser un ejemplo de denegación de servicio.**

c) Los ataques de denegación de servicio siempre provienen de una entidad ajena a la organización.

d) Todos los ataques de denegación de servicio se realizan mediante redes informáticas.

18) ¿Qué es un gusano informático?

**a) Un tipo de software malicioso que se propaga automáticamente sin la intervención de los usuarios.**

b) Un tipo de software malicioso que necesita intervención humana para propagarse.

c) Un tipo de software malicioso que muestra a los usuarios publicidad de forma intrusiva.

d) Un tipo de software malicioso que parece un programa inofensivo pero ocasiona daños al ser ejecutado.

19) ¿De qué modo se produce con más frecuencia la infección de los troyanos?

a) De forma automática, al navegar por Internet.

**b) Al ejecutar un archivo infectado.**

c) Al borrar un archivo infectado.

d) Todas las respuestas son correctas.

20) ¿Cuál de las siguientes opciones es cierta?

**a) El adware es un tipo de software malicioso que suele considerarse no dañino.**

b) Un keylogger es un tipo de software malicioso que cifra archivos del disco duro para exigir el pago de dinero.

c) La finalidad del spyware siempre es conseguir información del usuario para hacerle daño, por lo que se le considera un tipo de software malicioso dañino.

d) Un ransomware es un programa que muestra al usuario un mensaje indicándole que se va a formatear el disco duro sin que esto llegue a producirse.

21) Si recibimos un correo electrónico de un desconocido con un archivo adjunto que forma parte de una cadena de correos, ¿qué deberíamos hacer?

a) Pasar el antivirus al archivo adjunto para estar seguros de que no es peligroso y poder así ver su contenido.

**b) Ignorar el correo electrónico.**

c) Reenviar el correo a todos nuestros conocidos utilizando la copia oculta.

d) Reenviar el correo a todos nuestros conocidos utilizando la copia oculta y borrando la lista de correos originada por reenvíos previos.

22) ¿De qué modo se puede estar informado de las últimas amenazas de malware y conocer las últimas incidencias de seguridad detectadas?

a) Activando las actualizaciones de la herramienta antimalware.

**b) Visitando los centros de protección y respuesta ante amenazas.**

c) Activando las actualizaciones del sistema operativo y el navegador web.

d) Todas las respuestas son correctas.

23) ¿Por qué motivo son las suites de seguridad adecuadas para entornos empresariales?

a) Porque permiten intervenir remotamente en un equipo donde se ha detectado una infección que no se ha podido eliminar.

b) Porque permiten minimizar el consumo de ancho de banda.

c) Porque facilitan la gestión al tener centralizadas todas las actualizaciones.

**d) Todas las respuestas son correctas.**

24) ¿Por qué se dice que no existe una solución mágica ante una infección o incidente de seguridad?

a) Porque no existe ninguna herramienta antimalware que elimine todas las variedades de malware.

**b) Porque las medidas que se adoptan para desinfectar un equipo difieren según las diversas variantes y especímenes de malware de que se trate y, además, lo más común no siempre resulta efectivo.**

c) Porque debemos utilizar una herramienta distinta para eliminar correctamente cada infección o incidente de seguridad.

d) Porque conviene instalar muchas herramientas de detección y corrección de malware diferentes para tener un equipo seguro.

25) ¿Cuál de las siguientes afirmaciones sobre las políticas de los cortafuegos es verdadera?

a) Un cortafuegos con una política de entrada muy restrictiva es más seguro.

b) Un cortafuegos con una política de salida muy restrictiva es más seguro.

c) Un cortafuegos con políticas de entrada y salida muy restrictivas siempre es más conveniente.

**d) Ninguna de las respuestas es verdadera.**

26) ¿Cuál de las siguientes afirmaciones sobre los tipos de cortafuegos es verdadera?

a) Un cortafuegos de filtrado de paquetes tiene en cuenta la colocación individual de cada uno dentro de una serie de paquetes.

**b) Los cortafuegos de aplicación permiten que los programas y aplicaciones accedan o no a la red.**

c) Un cortafuegos de estado filtra el tráfico atendiendo únicamente a las direcciones IP, el protocolo y el número de puerto utilizado.

d) Todas las respuestas son verdaderas.

27) ¿Cuál de las siguientes afirmaciones sobre antivirus y suites de seguridad es cierta?

a) Se utilizan para denominar el mismo tipo de herramientas de seguridad.

**b) El término suite de seguridad engloba un conjunto de herramientas que protegen frente a diversos tipos de malware, como antivirus, antirootkits o antispyware, entre otros.**

c) Los antivirus ofrecen soluciones contra los virus y las suites de seguridad contra el resto de software malicioso.

d) Es mejor instalar un antivirus, ya que ofrece protección contra el tipo de malware más extendido: los virus.

28) ¿Qué herramienta utilizarías para proteger los datos importantes frente a pérdidas de información ocasionadas por malware?

**a) Copias de seguridad.**

b) Antivirus.

c) Cortafuegos.

d) Software congelador.

29) ¿Qué es un congelador?

a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.

b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.

c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.

**d) Un tipo de software que permite guardar el estado del equipo en un momento determinado, para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.**

30) ¿Cuál de las siguientes medidas no contribuye a protegerse contra el malware?

**a) Facilitar datos personales, como claves, por correo electrónico.**

b) Desactivar la interpretación de Visual Basic Script.

c) Actualizar periódicamente el sistema operativo y las aplicaciones críticas.

d) Mantenerse actualizado visitando periódicamente páginas web de información o suscribiéndose a boletines de seguridad.

31) ¿Qué se puede utilizar para realizar una recuperación de datos en un disco externo?

a) Clonezilla.

b) Rsync.

**c) GetDataBack.**

d) Los puntos de restauración.

32) La clonación de una partición a otra...

a) Consiste en copiar la partición en un archivo.

b) Copia todo el contenido de la partición en un disco.

c) No es posible con Clonezilla.

**d) Ninguna de las respuestas es correcta.**

33) ¿Qué implica una correcta gestión del almacenamiento de la información?

**a) Tener unas normas redactadas que indiquen cómo preservar la información.**

b) Conocer y detallar qué técnica de seguridad activa es la más adecuada para preservar la información.

c) Conocer y detallar qué técnica de seguridad pasiva es la más adecuada para preservar la información.

d) Tan solo mantener la información almacenada de forma segura ante fallos físicos.

34) ¿Cuál de los siguientes métodos no se corresponde con un método de recuperación de datos?

a) Gestión de imágenes.

b) Copia de seguridad.

**c) Tecnología NAS.**

d) Utilización de puntos de restauración.

35) Si un amigo te comenta que quiere instalar drivers nuevos para la tarjeta gráfica, pero que teme que luego el equipo no funcione correctamente, ¿qué le recomendarías para que el equipo pueda volver a funcionar en caso de que la instalación no resulte como debería?

a) Que se instale y configure un NAS.

b) Que copie los datos en un almacenamiento en la nube.

**c) Que cree un punto de restauración, si está utilizando Windows como sistema.**

d) Ninguna de las respuestas es válida.

36) El concepto de seguridad en sistemas de almacenamiento engloba:

a) Todas aquellas medidas que permitan mantener la información segura frente a fallos físicos

b) Todas aquellas medidas que permitan mantener la información segura frente a fallos lógicos

c) Protegerla de de accesos no autorizados

**d) Todas las anteriores son correctas**

37) Los puntos de restauración utilizados en Windows...

a) Permiten recuperar datos borrados de cualquier dispositivo de almacenamiento.

b) También son conocidos como modo a prueba de fallos.

c) Son similares a la aplicación de recuperación de datos GetDataBack.

**d) Permiten pasar a un estado anterior del sistema.**

38) ¿Cuál de las siguientes afirmaciones sobre los soportes o dispositivos para las copias de seguridad es cierta?

a) Para una correcta elección hay que tener en cuenta el tiempo de acceso a los datos.

b) Para una correcta elección hay que tener en cuenta la velocidad a la que se realizará la copia.

c) Para una correcta elección hay que tener en cuenta el tipo de datos.

**d) Las respuestas a y b son ciertas.**

39) ¿Cuál de los siguientes niveles de RAID sería el más apropiado para un sistema que necesite un rendimiento alto y en el que no son muy importantes las pérdidas de datos?

**a) RAID 0.**

b) RAID 1.

c) RAID 5.

d) RAID 6.

40) ¿Cuál de las siguientes afirmaciones es verdadera?

a) La tecnología NAS ofrece alojamiento en la nube.

**b) Los servicios de almacenamiento remoto ofrecen las modalidades de cloud público y cloud privado.**

c) Dentro de la clasificación de dispositivos locales encontramos los remotos y los de almacenamiento en la nube.

d) La tecnología SAN también es conocida como almacenamiento en la nube.

41) ¿Cuál es el primer paso que realiza un usuario en el proceso de solicitud de un certificado?

a) Generar una petición de certificado.

**b) Crear un par de claves.**

c) Firmar la solicitud.

d) Enviar la solicitud a la autoridad de certificación.

42) ¿En qué consiste la fase de saludo de SSL/TLS?

a) En intercambiar los nombres de las aplicaciones que se conectan.

b) En la presentación de los participantes en la comunicación.

**c) En el intercambio de claves públicas y la negociación del algoritmo de cifrado.**

d) En cifrar el tráfico con las claves intercambiadas previamente.

43) ¿Qué propiedad de la firma digital garantiza que el mensaje no ha sido modificado?

a) Autenticación.

**b) Integridad.**

c) No repudio.

d) Confidencialidad.

44) ¿Qué permite el mecanismo timestamping?

a) Saber la hora que es.

**b) Conocer el momento exacto en que se realizó la firma.**

c) Conocer el momento exacto en que se comprobó la firma.

d) Ninguna de las respuestas es correcta.

45) ¿Qué tipo de firma digital permite detectar cualquier cambio posterior de los datos firmados?

**a) Avanzada.**

b) Ordinaria.

c) Con árbitro.

d) Ninguna de las anteriores.

46) ¿Qué contiene un certificado digital?

a) El nombre del suscriptor.

b) El nombre de la autoridad de certificación que emite el certificado.

c) El método de firma.

**d) Todas las respuestas son correctas.**

47) ¿Qué requisito es necesario para poder comprobar la autenticidad de un certificado?

a) Tener actualizado el navegador.

b) Usar Mozilla Firefox.

**c) Tener instalado el certificado de la AC raíz en el navegador.**

d) Ninguna de las respuestas es correcta.

12) Si recibimos un mensaje de texto en nuestro teléfono que indica que se ha bloqueado nuestra tarjeta de crédito y que tenemos que visitar una página web para desbloquearla, es probable que estemos siendo víctimas de una técnica de suplantación de identidad conocida como...

a) Pharming.

b) Vishing.

**c) SMiShing.**

d) Grooming.

14) Al recibir un correo de un amigo nos llama la atención que el asunto del correo esté en inglés (ya que este amigo nunca nos escribe en este idioma). Además el correo solo contiene un enlace para visitar una página web. ¿Qué debemos hacer?

**a) Avisar a nuestro amigo de que es posible que haya sido víctima de una técnica de suplantación y es probable que tenga que cambiar la contraseña.**

b) Visitar la página web que nos proporciona el correo.

c) Reenviar el correo a nuestros amigos utilizando la copia oculta.

d) Eliminar el correo sin avisar a nuestro amigo.

16) Si en un equipo aparecen muchas ventanas de publicidad, ¿por qué variedad de software malicioso podemos deducir que se encuentra infectado?

a) Virus.

b) Gusano.

**c) Adware.**

d) Keylogger.

18) ¿Qué es un troyano?

a) Un tipo de software malicioso que se propaga automáticamente sin la intervención de los usuarios.

b) Un tipo de software malicioso que necesita intervención humana para propagarse.

c) Un tipo de software malicioso que muestra a los usuarios publicidad de forma intrusiva.

**d) Un tipo de software malicioso que parece un programa inofensivo pero que ocasiona daños cuando se ejecuta.**

19) ¿Cuál de las siguientes afirmaciones sobre el correo electrónico basura o spam es cierta?

a) Nunca tiene una intención comercial.

**b) Es un tipo de correo electrónico no deseado.**

c) Un correo electrónico que contiene una foto de un perrito jugando al futbol y que es enviado por un desconocido no se considera correo basura o spam, sin embargo sí se considera tal si se envía a 1000 personas.

d) Todas las opciones son ciertas.

20) ¿Cuál de las siguientes opciones es falsa?

a) Un rootkit es un tipo de software malicioso que utiliza técnicas para permanecer oculto respecto al sistema.

**b) El hecho de descargar un programa de la página web oficial garantiza que este no es software malicioso.**

c) Conviene desconfiar del software que circula por las redes P2P porque desconocemos su procedencia.

d) Algunas variedades de malware utilizan el correo electrónico para propagarse.

21) ¿Cuál de las siguientes afirmaciones es cierta?

a) Las copias de seguridad permiten evitar infecciones de virus y malware.

b) Las copias de seguridad permiten evitar que nuestro equipo se infecte al navegar por Internet.

**c) Las copias de seguridad permiten minimizar el impacto ocasionado por el malware.**

d) Las copias de seguridad contribuyen a la desinfección de malware del equipo.

22) ¿Qué tipo de suite de seguridad será más adecuada en un entorno compuesto por 10 equipos?

a) Suite de seguridad personal.

**b) Suite de seguridad corporativa.**

c) Suite de seguridad compleja.

d) Suite de seguridad.

24) ¿Qué herramienta utilizarías para bloquear accesos no autorizados a tu equipo?

**a) Cortafuegos.**

b) Copias de seguridad.

c) Software congelador.

d) Antispyware.

25) ¿Cuál de las siguientes medidas contribuye a protegerse del malware?

a) Diseñar políticas de contraseñas que incluyan contraseñas complejas.

b) No navegar por páginas web inseguras, sospechosas o que ofrezcan regalos o promociones dudosos.

c) Utilizar cuentas de usuario con privilegios limitados para el uso diario del equipo.

**d) Todas las respuestas son correctas.**

26) ¿Cuál de los siguientes servicios no se ofrecen en un centro de protección y respuesta ante amenazas?

a) Propagación de herramientas para eliminar malware.

b) Análisis de vulnerabilidades detectadas y de incidentes de seguridad.

c) Avisos de seguridad.

**d) Ninguno de los anteriores.**

27) ¿Qué tipo de cortafuegos permite bloquear y permitir el tráfico que llega a un equipo informático?

a) Cortafuegos perimetral.

b) Cortafuegos de red.

**c) Cortafuegos de host.**

d) Cortafuegos individual.

28) ¿Cuál de las siguientes medidas contribuye a protegernos contra el malware en correos electrónicos?

a) Configurar el correo para que compruebe los mensajes.

b) No reenviar mensajes que formen parte de cadenas.

c) No hacer clic en los enlaces que aparecen en un correo electrónico que procede de una fuente que no es de confianza.

**d) Todas las respuestas son correctas.**

29) ¿Qué nombre recibe el conjunto de herramientas que contribuye a prevenir las infecciones por malware y a desinfectar los equipos infectados?

**a) Suite de seguridad.**

b) Programas de control parental.

c) Cortafuegos.

d) Copias de seguridad.

30) ¿Qué inconveniente puede presentar la utilización de software congelador para restaurar un equipo al mismo punto?

**a) Si el sistema se restaura al mismo punto, no se actualiza el sistema, por lo que será vulnerable a futuras amenazas.**

b) Este tipo de herramienta no es adecuado si se permite la utilización de dispositivos de almacenamiento externos.

c) Un usuario malintencionado no puede acceder a información previa a la sesión actual.

d) Se protege de las infecciones por software malicioso.

32) ¿Cuál de las siguientes aplicaciones utilizaremos para crear una imagen?

**a) Clonezilla.**

b) Rsync.

c) GetDataBack.

d) Los puntos de restauración.

33) ¿Cuál de las siguientes afirmaciones sobre los puntos de restauración creados con Windows es correcta?

a) Se utilizan para restaurar el equipo cuando el sistema operativo no arranca.

**b) Uno de los inconvenientes que presenta su uso es la cantidad de espacio que se necesita para almacenar los puntos.**

c) Se deben crear puntos de restauración diariamente para su óptima utilización.

d) Ninguna de las afirmaciones es correcta.

34) ¿Cuál de las siguientes afirmaciones sobre RAID 5 es correcta?

a) Necesita dos discos, por tanto la información almacenada se duplica de un disco al otro.

**b) Se puede implementar con tres discos, entre los cuales se reparte en bandas la información.**

c) Su funcionamiento es similar al de RAID 1.

d) Recibe también el nombre de disk mirroring.

35) ¿Cuál de las siguientes afirmaciones sobre la gestión de imágenes es verdadera?

a) El tipo de imagen que más se suele utilizar es el de tipo incremental.

b) La clonación en equipos solo puede realizarse si se trata de una clonación de disco a disco y estos son iguales en características.

**c) Si el equipo no arranca, su restauración a partir de una imagen es una solución.**

d) Si el equipo ni siquiera arranca, la restauración mediante una imagen no es una buena solución.

37) Si un amigo te comenta que posee mucha información y que le gustaría disponer de un sistema que le permitiera, en caso de fallo del disco, recuperar la información de manera rápida y en cualquier situación, ¿qué le recomendarías en primer lugar?

**a) Que se compre otro disco y configure un sistema RAID 1.**

b) Que cree una imagen al instalar el sistema operativo.

c) Que copie los datos en un almacenamiento en la nube.

d) Que cree un punto de restauración.

38) ¿Cuál de las siguientes afirmaciones es falsa?

a) Para solucionar la necesidad de espacio de almacenamiento no siempre es recomendable ampliar el número de discos duros.

b) Existen distribuciones software que permiten transformar un equipo en servidor NAS.

c) La tecnología SAN es una red de área de almacenamiento.

**d) El almacenamiento en la nube ofrece balanceo de carga y tolerancia a fallos.**

40) ¿Cuál de las siguientes afirmaciones sobre copias de seguridad es cierta?

a) Las copias de seguridad en frío son aquellas que se hacen sobre ficheros abiertos y bases de datos sobre las que se está trabajando.

b) Las copias de seguridad en caliente son aquellas que se hacen sobre ficheros y bases de datos sobre las que no hay accesos.

c) No se permite realizar copias en caliente si se utilizan dispositivos de almacenamiento locales.

**d) Ninguna de las respuestas es cierta.**

1) ¿Qué se creó para solucionar el problema de la confianza en la clave pública de un usuario?

a) Las funciones hash.

b) Las listas blancas.

**c) Los certificados digitales y las autoridades de certificación.**

d) Ninguna de las respuestas es correcta.

2) ¿Qué propiedad de la firma digital no permite que el emisor pueda negar la autoría de un mensaje?

a) Autenticación.

b) Integridad.

**c) No repudio.**

d) Confidencialidad.

3) ¿Para qué se utiliza Diffie-Hellman?

a) Para cifrar sesiones SSL/TLS.

b) Para informar al usuario de que el certificado del servidor no es válido.

c) Para verificar el certificado del servidor.

**d) Ninguna de las respuestas es correcta.**

5) ¿Qué acción debe realizarse para comprobar la validez de un certificado?

a) Validarlo en la web de la autoridad de certificación que lo ha firmado.

b) Mirar si la fecha actual es mayor que la de caducidad del certificado.

**c) Verificar la firma de la autoridad que ha firmado el certificado.**

d) No ha de realizarse ninguna acción.

6) ¿Qué se recomienda a la hora de usar cifrado en una unidad de disco USB?

a) Utilizar siempre Linux.

**b) Crear un volumen o contenedor dentro del dispositivo.**

c) Que esté formateado en NTFS.

d) Que tenga un tamaño menor de 16 GB.

12) ¿Qué es el ransomware?

a) Un tipo de software malicioso considerado no dañino.

b) Un tipo de software malicioso que utiliza técnicas especiales para permanecer oculto respecto al sistema.

c) Un tipo de software malicioso que muestra al usuario un mensaje indicándole que se va a formatear el disco duro sin que esto llegue a producirse.

**d) Ninguna de las opciones anteriores es cierta.**

13) ¿Cómo se podrían disminuir los fraudes informáticos derivados de las cadenas de correos electrónicos?

a) Evitando reenviar el correo en cualquier caso.

b) Reenviando el correo íntegramente solo a algunos amigos.

**c) Utilizando, en caso de que se decida reenviar el correo, la copia oculta (campo CCO) y eliminando la lista de remitentes anteriores.**

d) Reenviando el correo recibido a todos los contactos conocidos.

15) ¿Qué es un virus?

a) Un tipo de software malicioso que puede duplicarse por sí mismo sin necesidad de infectar otros archivos.

**b) Un tipo de software malicioso que se propaga infectando otros ficheros.**

c) Un tipo de software malicioso que muestra a los usuarios publicidad de forma intrusiva.

d) Un tipo de software malicioso que parece un programa inofensivo pero que ocasiona daños cuando se ejecuta.

16) ¿Cuál de las siguientes afirmaciones relacionadas con la suplantación de identidad es cierta?

a) El phishing es un tipo de estafa informática que emplea técnicas de ingeniería social para suplantar la identidad de otra persona o entidad haciéndose pasar por ella mediante el protocolo de voz sobre IP.

b) El SMiShing es un tipo de estafa informática que hace creer a la víctima, sin que sea realmente así, que se ha comprometido su seguridad.

c) El SMiShing es un tipo de estafa informática que utiliza mensajes de correo basura o spam para embaucar a las víctimas.

**d) Ninguna de las opciones anteriores es cierta.**

18) ¿Cuál de las siguientes opciones constituye un ejemplo de denegación de servicio?

a) Un empleado instala a propósito en un equipo de la empresa un programa que genera tráfico basura y consume mucho ancho de banda, impidiendo que el resto de usuarios de la red ejerza un uso normal de la misma.

b) Juan ejecuta un archivo adjunto en un correo que, sin saberlo, instala un programa malicioso que afecta al funcionamiento del servidor de correo de ese equipo.

c) Un atacante que controla un gran número de equipos informáticos realiza un ataque coordinado contra un servidor web para detener su funcionamiento.

**d) Todas las opciones anteriores son ejemplos de denegación de servicio.**

22) ¿Qué opción de las siguientes adoptarías para evitar infecciones al navegar por Internet?

a) Instalar una suite de seguridad que ofrezca inspección de tráfico en tiempo real.

**b) Hacer una copia de seguridad de todos los archivos importantes del sistema.**

c) Configurar el cortafuegos para rechazar todo el tráfico entrante.

d) Instalar un software congelador.

24) ¿Qué es una copia de seguridad?

**a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.**

b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.

c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado, para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

27) ¿Qué ventajas presenta la utilización de software congelador?

a) El equipo que utiliza este tipo de herramientas estará libre de virus de forma garantizada.

**b) Cuando se produce la restauración, se eliminan las infecciones previas originadas por software malicioso.**

c) La información generada por un usuario en cada sesión no será modificada al restaurar el equipo.

d) Ninguna de las respuestas es correcta.

28) ¿Qué es un cortafuegos?

a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.

**b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.**

c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado, para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

29) Nuestro equipo parece infectado por algún tipo de malware que nuestra herramienta antimalware es incapaz de eliminar, ya que continuamente aparece una ventana que indica que se ha detectado una actividad ilegal procedente de este equipo y que debemos pagar una multa a una cuenta de correo. ¿Qué deberíamos hacer?

a) Formatear el equipo para eliminarlo, aunque perdamos información importante de la que no tengamos copia de seguridad.

b) Si nuestro antivirus no lo puede detectar, desinstalarlo y probar otro antivirus mejor.

c) Pagar la multa.

**d) Visitar las páginas web de los centros de protección y respuesta ante amenazas para estudiar si nos encontramos ante algún tipo de estafa.**

34) ¿Se puede garantizar una buena gestión del almacenamiento de la información?

**a) Sí, siempre que se cumplan las normas de la política de almacenamiento.**

b) Sí, siempre que se mantenga la información alejada de accesos no autorizados.

c) Sí, siempre que se garantice una seguridad activa de la información.

d) Ninguna de las respuestas es correcta.

35) ¿Cuál de los siguientes niveles de RAID sería el más adecuado para un entorno doméstico en el que se necesita principalmente tolerancia a fallos?

a) RAID 0.

**b) RAID 1.**

c) RAID 5.

d) Las respuestas a y b son adecuadas.

36) ¿Cuál de las siguientes afirmaciones sobre la tecnología RAID es cierta?

**a) No es apta para la recuperación de datos.**

b) Se considera una medida preventiva.

c) En caso de pérdida de datos en un disco, para recuperar los datos es suficiente con transferir la estructura y el contenido del disco.

d) Permite volver a un estado anterior del sistema para proceder a la recuperación.

40) ¿En cuál de las siguientes situaciones es interesante utilizar la gestión de imágenes?

**a) Cuando, tras instalar algún programa o actualización, el sistema empieza a funcionar de forma no deseada.**

b) Cuando es necesario recuperar los datos de un disco externo formateado.

c) Cuando, por culpa de un virus, se han borrado los datos del dispositivo de almacenamiento USB.

d) Ninguna de las respuestas es correcta.

1) ¿De qué tipo es el sistema que permite el intercambio de claves en SSL/TLS?

**a) Híbrido.**

b) Simétrico.

c) Asimétrico.

d) Ninguna de las respuestas anteriores es correcta.

3) En el proceso de firma digital de un documento, obtener el resumen del documento es...

a) El último paso.

b) El segundo paso.

**c) El primer paso.**

d) Un paso opcional.

10) ¿Cómo se llama la fase inicial en la que se negocia el algoritmo de cifrado a usar en una conexión SSL/TLS?

a) Fase de despedida.

b) Fase de negociación.

c) Fase de intercambio de claves.

**d) Fase de saludo.**

17) ¿Cuál de las siguientes opciones es cierta?

a) Un espécimen de software malicioso puede realizar más de una acción dañina, como capturar las pulsaciones del teclado y utilizar técnicas para permanecer oculto respecto al sistema.

b) Ransomware es un tipo de software malicioso que cifra archivos del disco duro para exigir el pago de dinero.

c) Una bomba lógica es un tipo de software malicioso que se pone en funcionamiento cuando se cumple alguna condición.

**d) Todas las respuestas son ciertas.**

19) ¿Cuál de las siguientes afirmaciones sobre el correo electrónico no deseado y el correo basura o spam es cierta?

a) Ambos son lo mismo.

b) Un correo electrónico que contiene publicidad de una empresa y que es enviado por un desconocido se considera correo no deseado, sin embargo si quien lo envía es un conocido que nos cae mal se considera correo basura o spam.

**c) El correo basura o spam es un tipo concreto de correo electrónico no deseado cuyos fines son publicitarios o económicos.**

d) El correo electrónico no deseado es un tipo concreto de correo basura o spam cuyos fines son publicitarios o económicos.

20) ¿Cómo se denomina un programa que parece inofensivo pero que permite a otro usuario controlar nuestro equipo de forma remota?

a) Gusano.

**b) Troyano.**

c) Rogueware.

d) Rootkit.

21) Tenemos un programa que requiere acceso a Internet y que utiliza un puerto TCP diferente cada vez que se ejecuta. ¿Cuál de los siguientes tipos de cortafuegos sería más adecuado utilizar y cómo lo configurarías?

a) Cortafuegos de filtrado de paquetes, permitiendo la entrada de paquetes que lleguen a cualquier puerto TCP.

b) Cortafuegos de filtrado de paquetes, permitiendo la salida de paquetes procedentes de cualquier puerto TCP.

**c) Cortafuegos de aplicación, permitiendo el acceso a esa aplicación.**

d) Ninguno de los anteriores.

22) ¿Cuál de las siguientes medidas no contribuye a protegernos contra el malware en correos electrónicos?

a) Denunciar el correo abusivo o fraudulento informando al emisor del mensaje.

**b) Configurar el antivirus para que inspeccione el correo electrónico, ya que así estaremos seguros de que no hay ningún tipo de malware y podremos confiar en el contenido de los correos.**

c) Cuando reenviemos correos de forma masiva, borrar la lista de direcciones proveniente de reenvíos anteriores.

d) Utilizar la copia oculta al reenviar correos..

29) ¿Cuál de las siguientes afirmaciones sobre los cortafuegos es cierta?

a) Los cortafuegos permiten o deniegan el tráfico en función de las reglas que deben cumplir los mensajes que pasan por ellos.

b) Los cortafuegos suelen definir una política por defecto que se aplica a aquellos mensajes que no cumplen las condiciones de ninguna regla.

c) Un cortafuegos correctamente configurado añade protección a la red o al equipo, pero debe combinarse con otras herramientas de protección.

**d) Todas las respuestas son ciertas.**

30) ¿Qué debo hacer si sospecho que mi equipo está infectado por algún tipo de malware?

a) Escanear el equipo en busca de virus.

b) Restaurar el sistema a un estado anterior para eliminarlo.

c) Hacer copias de seguridad para evitar que ese malware elimine mis archivos importantes.

**d) Antes de realizar nada, identificar de qué tipo de malware se trata y cuál es su alcance.**

33) ¿Qué se puede utilizar para recuperar los datos de un disco duro formateado por error?

**a) La herramienta GetDataBack.**

b) La restauración de la imagen del equipo que viene de fábrica.

c) Los puntos de restauración creados en Windows para recuperar cualquier sistema operativo que esté instalado.

d) Todas las respuestas con correctas.

34) Si alguien te comenta que teme perder las fotos de su familia que tiene almacenadas en un disco externo, ¿qué le recomendarías para mantener la integridad de la información?

**a) Que haga copias de seguridad periódicamente.**

b) Que se haga una imagen del disco y la guarde en un lugar seguro.

c) Que cree un punto de restauración mensualmente.

d) Ninguna de las respuestas es válida.

39) ¿Qué hay que tener en cuenta para llevar a cabo un buen control sobre el amacenamiento de la información?:

a) Que se garantice una seguridad física

b) Que se garantice una seguridad lógica

c) Que se permite mantener la disponible, la integridad y la autenticidad de la información

**d) Todas las afirmaciones anteriores son correctas**

40) ¿Cuál de las siguientes afirmaciones sobre copias de seguridad es verdadera?

a) Las copias normales copian los archivos creados en el día.

b) Para datos muy cambiantes es recomendable hacer una copia de los mismos trimestralmente.

**c) La política de retención indica cuánto tiempo se va a conservar cada copia de seguridad.**

d) Podrá utilizarse el mismo tipo de copia tanto si se van a copiar bases de datos completas como ficheros ordinarios.

9) ¿Cuál de los siguientes es un elemento hardware necesario para usar el DNIe?

a) Teclado QWERTY.

**b) Lector de tarjetas inteligentes.**

c) Ratón.

d) Lector de CD-ROM.

16) Nuestro equipo será más vulnerable si...

a) El sistema operativo no se actualiza periódicamente.

b) El navegador y los plugins que utiliza no están actualizados.

c) No actualizamos los programas que instalamos en él.

**d) Todas las respuestas son correctas.**

17) ¿Cuál de las siguientes opciones es verdadera?

a) Todo software malicioso realiza acciones consideradas dañinas o perjudiciales.

b) Según el impacto producido en la víctima diferenciamos entre especímenes que se instalan de forma automática y especímenes que necesitan la intervención del usuario.

c) Según las acciones que realiza un virus distinguimos entre virus automático y virus residente.

**d) Algunas variedades de software malicioso pueden realizar más de una acción.**

20) ¿Cuál de las siguientes afirmaciones acerca de la ingeniería social aplicada a la informática es cierta?

a) El correo electrónico es tal vez el medio más utilizado por los estafadores, aunque no el único.

b) Los piratas informáticos suelen utilizar técnicas de ingeniería social para suplantar la identidad de las víctimas.

c) Los correos electrónicos masivos son considerados otra técnica de ingeniería social.

**d) Todas las opciones anteriores son ciertas.**

21) ¿Cuál de las siguientes afirmaciones sobre suites de seguridad corporativas es cierta?

a) Permiten que un equipo se descargue la última versión del motor y la base de firmas y que el resto de equipos se la descarguen de aquel, pero no permiten analizar otro equipo de la red.

b) Constituyen la solución más adecuada para todas las situaciones, incluso para un solo equipo.

**c) Permiten obtener información relativa a software malicioso detectado o eliminado en los clientes de la red.**

d) Todas las respuestas son ciertas.

25) ¿Qué herramienta recomendarías emplear en un aula de informática donde se permite la utilización de USB y la instalación de programas, lo que puede ocasionar muchas infecciones por malware?

a) Un navegador actualizado.

b) Un cortafuegos muy restrictivo.

c) Un cortafuegos permisivo.

**d) Un software congelador.**

26) ¿Qué servicios ofrecen los centros de protección y respuesta ante amenazas?

a) Propagación de información relacionada con la seguridad.

b) Auditorías de seguridad.

c) Gestión de vulnerabilidades.

**d) Todas las respuestas son correctas.**

27) ¿Qué es una suite de seguridad?

a) Una medida de seguridad paliativa que consiste en guardar una parte o toda la información del sistema con la intención de poder recuperarla en caso de pérdida de información.

b) Un dispositivo software o hardware que forma parte de un equipo y está diseñado para protegerlo mediante el bloqueo de accesos no autorizados.

**c) Un conjunto de programas de seguridad que contribuyen a la detección de software malicioso y, en muchos casos, a su desinfección.**

d) Un tipo de software que permite guardar el estado del equipo en un momento determinado para que, al volver a iniciarse el equipo, el estado se restaure automáticamente.

35) ¿Qué implica una correcta gestión del almacenamiento de la información?

a) Saber cuánta capacidad se va a necesitar.

b) Conocer con qué frecuencia se va a utilizar.

c) Estudiar qué tecnología de almacenamiento será la más adecuada.

**d) Todas las respuestas son correctas.**